

NIMIS Pentesting Services Agreement

Version 1.8 – Last updated: 3 August 2026

1. The parties and acceptance

This NIMIS Pentesting Services Agreement ("**Agreement**") is entered into between:

- **NIMIS Cybersecurity Pty Ltd, ABN 25 619 710 655** ("**NIMIS**", "**we**", "**us**", "**our**"); and
- the individual or entity that accepts this Agreement or uses the Services ("**Client**", "**you**", "**your**").

You accept this Agreement by clicking to accept it, by enrolling an application for testing, or by running or authorising a Test, whichever occurs first. If you accept on behalf of an organisation, you represent and warrant that you are authorised to bind that organisation, and "**Client**" means that organisation. If you do not agree, you must not enrol any application or run any Test.

This Agreement governs your use of the NIMIS penetration-testing platform, dashboard, APIs, and related security-testing services ("**Services**"). It prevails over the general *Terms of Service* to the extent of any inconsistency in relation to the Services.

2. Definitions

- "**Test**" means a single penetration-testing engagement or run initiated through the Services against a Target.
- "**Target**" means a web application, API domain, host, or endpoint that the Client has enrolled and that NIMIS has verified as owned or controlled by the Client under clause 4.
- "**Ownership Verification**" means the mechanism described in clause 4 by which the Client demonstrates control of a Target before any Test runs.
- "**Findings**" means the reports, evidence, vulnerability records, and other outputs produced by a Test.

- **"Fees"** means the amounts payable for the Services under clause 15, including per-Test and subscription charges.
- **"Authorised Scope"** means the set of verified Targets against which the Client has authorised testing, together with any scope limits configured for a Test.
- **"Authorised User"** means an individual, such as an employee or contractor of the Client, whom the Client permits to access and use the Services on its behalf through the Client's account.
- **"Tested Entity"** means the entity that owns, controls, or operates the systems, applications, networks, or assets that are the subject of the Services, whether that entity is the Client or a third party for whom the Client procures the Services.
- **"Restricted Jurisdiction"** means each of Singapore, Malaysia, Ghana, the People's Republic of China, and the Kingdom of Saudi Arabia, and any further jurisdiction notified by NIMIS to the Client in writing from time to time.

3. The Services

NIMIS provides an automated, autonomous penetration-testing platform that discovers, probes, and actively tests web applications and APIs for security vulnerabilities, and produces Findings. The Services are **active and intrusive** by design: they send real attack traffic to the Target. The Services do **not** perform volumetric denial-of-service or distributed-denial-of-service (DoS/DDoS) testing, and must not be used or configured in an attempt to do so.

The Client controls and can limit what is tested (see clause 6), and may stop a running Test at any time using the stop control in the dashboard.

NIMIS grants the Client a limited, non-exclusive, non-transferable, non-sublicensable right to use the Services during the term, solely for the Client's own internal security purposes and strictly within the Authorised Scope.

4. Ownership and verification of Targets

No Test runs against a Target until ownership of that Target has been verified. The Client must complete Ownership Verification for each Target before its first Test:

- **Web application:** by publishing a NIMIS-issued verification meta tag (`<meta name="nimis-verify" content="[verification-token]">`) on the application's primary URL; and

- **Each API domain:** by serving the verification token as `text/plain` from `GET https://<api-host>/<base-path>/nimis-verify`.

All verification material must be served over HTTPS. NIMIS checks for the verification material before the first Test runs, and testing is confined to the verified web-app host and verified API host/path combinations. The NIMIS backend is authoritative as to whether verification has succeeded.

Ownership Verification is a **technical control**, not a warranty by NIMIS of your legal rights. Verifying control of a Target does **not** relieve you of, and is **not** a substitute for, your obligations and warranties under clause 5. Control of a Target's DNS, hosting, or content does not by itself establish that you are legally entitled to have it tested.

5. Client authorisation and warranties: you may only test what you own or are authorised to test

This clause is fundamental to the Agreement and is a condition of it. You represent, warrant, and covenant, on a continuing basis, that for every Target you enrol and every Test you initiate or authorise:

- **(a) Ownership or control.** You own the Target, or you otherwise legally control it and are entitled to have it tested.
- **(b) Authorisation.** You have full authority and all necessary rights, consents, licences, and permissions to authorise penetration testing of the Target, and you hereby authorise NIMIS to conduct such testing within the Authorised Scope. **You are solely responsible for ensuring you have permission to test.**
- **(c) Third-party permissions.** Where the Target is hosted by, or depends on, third parties (for example, a cloud or hosting provider, CDN, WAF, or managed service), you have obtained any authorisation, notification, or clearance those third parties require for penetration testing under their acceptable-use or testing policies, and you will comply with those policies.
- **(d) No third-party or unauthorised systems.** You will not enrol, submit, direct, or configure the Services to test any system, application, domain, data, account, or infrastructure that you do not own or are not authorised to test, and you will not use the Services to test on behalf of any third party except as permitted under clause 14.
- **(e) Lawfulness.** Your use of the Services, and the testing you authorise, complies with all applicable laws, including computer-misuse, unauthorised-access, privacy, and data-

protection laws in every jurisdiction connected with the Target and its data.

- **(f) Accuracy and maintenance.** The application details, API domains, credentials, and scope information you provide are accurate and current, and you will keep verification material in place for the duration of testing.
- **(g) Evidence of authorisation on request.** You will, on NIMIS's request, promptly provide written evidence reasonably satisfactory to NIMIS of your authority to have a Target tested (including, where the Tested Entity is not the Client, evidence of the Tested Entity's authorisation). NIMIS may suspend or decline any Test or enrolment until such evidence is provided, without liability to the Client. NIMIS's right to request evidence does not create any obligation on NIMIS to verify, and does not dilute your sole responsibility under this clause 5.

You acknowledge that NIMIS relies on these warranties, that NIMIS cannot independently determine your legal right to test a Target beyond the technical Ownership Verification, and that **you bear sole responsibility for the authorisation of every Test**. A breach of this clause 5 is a material breach that is not capable of cure.

6. Client responsibilities and safe testing

You are responsible for the environment you choose to test, and for defining and limiting what is tested. You agree to:

- take and maintain **current, restorable backups** of any Target and its data before a Test runs, and have a rollback plan;
- ensure appropriate change-management, monitoring, and stakeholder awareness are in place for the testing window;
- provide accurate scope, credentials, and configuration, and use the scope controls the Services make available: you set and limit the Authorised Scope through the enrolled web-application URL and API domains, and refine it using allowed-path and denied-path rules to include or exclude specific areas of a Target;
- stop a Test yourself using the stop control in the dashboard if you need testing to end early;
- promptly disable or de-scope a Target you no longer own or are no longer authorised to test.

Test credentials. Where you provide credentials so the Services can perform authenticated testing (for example, test-account usernames, passwords, PINs, or authenticator secrets), you represent and warrant that you are entitled to provide them for this purpose. You should provide **dedicated, least-privilege, non-production test accounts** rather than privileged, personal, or

production credentials. You are responsible for the accounts you supply and for the consequences of the access they grant. You control these credentials and can update or remove them at any time through the dashboard. NIMIS's handling of the credentials you provide is described in clause 12.

Authorised Users. The Client may permit its Authorised Users to access and use the Services on its behalf. The Client is **responsible for all acts and omissions of its Authorised Users** in connection with the Services as if they were the Client's own, and will **ensure that each Authorised User complies with this Agreement**, including the authorisation and ownership obligations in clause 5, the acceptable-use and other restrictions in clause 14, and the confidentiality obligations in clause 11. The Client is responsible for provisioning, controlling, and promptly revoking Authorised User access (including when an individual no longer requires it or ceases to be engaged by the Client), and for keeping account credentials secure. The Client's representations, warranties, indemnity, and other obligations under this Agreement apply to anything done through the Client's account by an Authorised User. For the avoidance of doubt, an Authorised User is not required to enter into this Agreement in their personal capacity, and nothing in this Agreement makes an Authorised User a party to it.

7. Production testing: strongly discouraged; the Client's choice and the Client's risk

NIMIS strongly recommends that you test only in a dedicated test or staging environment, and strongly discourages testing against production systems. Production testing risks impacting real users, live data, and live services.

If you nevertheless choose to enrol, configure, or run a Test against a production environment, you do so **entirely at your own election and your own risk**. You acknowledge and agree that:

- **(a)** the decision to test production, rather than a staging or test environment, is yours alone and is made against NIMIS's express recommendation;
- **(b)** NIMIS does not select your environment, cannot know whether a given Target is production, and relies on you to choose an appropriate environment;
- **(c)** you accept full responsibility for all consequences of testing production, including any data modification, data loss, corruption, outage, degradation, or disruption to your systems, your users, or third parties; and

- **(d)** to the maximum extent permitted by law, and subject to clauses 19 and 21, NIMIS has no liability for any loss or damage arising from your choice to test a production environment.

This clause operates in addition to, and does not limit, the acknowledgment and assumption of risk in clause 8.

8. Acknowledgment and assumption of risk

You acknowledge and accept that penetration testing is inherently risky. By enrolling an application and running a Test, you confirm your understanding that the Services actively probe the Target and **can cause data modification, creation of database entries, corruption or deletion of data, degraded performance, service disruption, and outages**, and that these effects can occur even when the Services operate correctly. This mirrors the acknowledgment you accept in the NIMIS dashboard when adding an application (*"I understand the risks and accept responsibility for this test environment"*).

You voluntarily assume these risks. To the maximum extent permitted by law, and subject to clauses 19 and 21, NIMIS is not liable for, and you release NIMIS from, any loss or damage arising from the intended, active operation of the Services against a Target you have authorised (including data modification, disruption, downtime, or consequential effects on the Target, its data, or its users) where NIMIS has operated the Services substantially as designed.

9. Nature and limits of testing: point-in-time; scope, tooling, and time

You acknowledge and agree that penetration testing is subject to inherent limitations, and that the following are fundamental assumptions on which NIMIS provides the Services:

- **(a) Bounded by scope.** A Test assesses only the Authorised Scope, as enrolled, verified, and configured. Anything outside that scope is not assessed.
- **(b) Bounded by tooling and technique.** The Services are automated and assess a Target using the techniques, coverage, and capabilities available to the platform. No tool or methodology can identify every vulnerability, misconfiguration, or weakness.
- **(c) Bounded by time.** A Test is performed within a finite time window. Additional time or different conditions may surface issues not found within that window.
- **(d) Reasonable efforts, not a guarantee.** NIMIS makes reasonable efforts to test the Authorised Scope as fully as the platform allows, but **does not guarantee that a Test will**

identify all, or any, vulnerabilities, and gives no warranty of completeness.

- **(e) Point-in-time.** A Test and its Findings describe the Target only as it existed at the time of the Test. **Any change to the Target, its environment, dependencies, configuration, data, or surrounding systems after a Test may change its security posture and render the Findings inaccurate or out of date.** Findings should not be relied on as reflecting the current state of a changed environment.
- **(f) Not a certification. The absence of Findings is not a certification, warranty, or guarantee that a Target is secure or free of vulnerabilities.** Findings are informational, depend on scope, inputs, timing, and conditions, and do not constitute legal, compliance, or professional advice.
- **(g) Client's own programme.** The Services are one input into the Client's security programme and are not a substitute for it. Any decision to remediate, retest, or accept risk remains the Client's.

10. Findings, intellectual property, and licence

As between the parties, the Client owns the Findings relating to its Targets. NIMIS grants the Client a perpetual, worldwide licence to use the Findings for the Client's internal security and compliance purposes. NIMIS retains ownership of the Services, the platform, testing engines, models, methodologies, and any underlying or derived technology, and may use de-identified, aggregated data to operate and improve the Services. **NIMIS does not use the Client's applications, test traffic, or Findings to train NIMIS's models.**

The Client acquires **no right, title, or interest** in the Services, platform, testing engines, models, algorithms, methodologies, know-how, or any underlying or derived technology, and **no licence is granted by implication, estoppel, or otherwise** except the limited rights expressly granted in this Agreement. NIMIS's methods, models, and the manner in which the Services and any Test are performed are **NIMIS's Confidential Information and trade secrets**, and NIMIS is **under no obligation to disclose or explain how the Services, the platform, or any Test operate, detect, or produce results.**

11. Confidentiality

Each party may receive confidential information of the other. Each party will protect the other's confidential information with at least reasonable care, use it only to perform this Agreement, and

not disclose it except to personnel and contractors who need it and are bound by confidentiality obligations, or as required by law. Findings and Target vulnerability data are Client confidential information.

Exclusions. Confidential information does not include information that: (a) is or becomes public otherwise than through a breach of this clause; (b) was rightfully known to the receiving party, free of any obligation of confidence, before disclosure; (c) is rightfully received from a third party without restriction and without breach of any obligation of confidence; or (d) is independently developed by the receiving party without use of or reference to the other party's confidential information.

Compelled disclosure. If the receiving party is required by law, regulation, a court, or a regulator to disclose the other party's confidential information, it may do so, but (where lawful and reasonably practicable) must first give the other party prompt written notice, disclose only the portion it is legally required to disclose, and provide reasonable cooperation, at the other party's request and cost, so that party can seek a protective order or confidential treatment.

Return or destruction. On termination of this Agreement, or on the disclosing party's written request, the receiving party will, at the disclosing party's option, return or securely destroy the other party's confidential information in its possession or control, except to the extent retention is required by law or under clause 15(f), or the information is held in routine, not-readily-accessible backups that remain subject to this clause until deleted in the ordinary course. NIMIS's deletion of Client data under clause 15(f) satisfies this obligation for that data.

Survival. The obligations in this clause continue for **three (3) years** after termination of this Agreement, and **indefinitely** for any information that constitutes a trade secret for so long as it remains a trade secret under applicable law.

12. Data protection, security, and breach notification

NIMIS handles personal data in accordance with its Privacy Policy and, where NIMIS processes personal data on the Client's behalf, any applicable **Data Processing Addendum (DPA)**. NIMIS does not require, and does not intend to collect or create, personal data through testing, and **personal data should not be present in a test environment**. The Client is responsible for ensuring that any personal data present in a Target has a lawful basis, and acknowledges that active testing may nonetheless access, alter, or generate records within the Target (which the Client should assume may include personal data where the Client has placed it there).

Security. NIMIS applies administrative, technical, and physical safeguards consistent with recognised information-security practices (such as those reflected in ISO/IEC 27001) to protect Findings and Client-provided information. These include personnel background and confidentiality checks, secure and access-controlled data-centre infrastructure, least-privilege access controls, and encryption of data in transit and at rest. Credentials the Client provides for authenticated testing are used **solely** to perform the Client's Tests, are held securely and encrypted at rest, and can be updated or removed by the Client at any time through the dashboard. Consistent with clause 10, the specific security measures, tooling, and architecture NIMIS uses are NIMIS's Confidential Information, and this clause does not require NIMIS to disclose them. This clause describes NIMIS's security practices and does **not** create any warranty beyond clause 16.

Breach notification. If NIMIS becomes aware of a confirmed security breach affecting the Client's Findings or other Client-provided information held by NIMIS, NIMIS will notify the Client's account owner (the individual who registered the account) by email without undue delay, together with such information as NIMIS is reasonably able to provide. Any such notice is provided in good faith, is **not** an admission of fault or liability, and does not expand NIMIS's liability beyond clause 17. This obligation is in addition to any personal-data breach obligations under the DPA, which govern where they apply.

13. Jurisdiction Warranty

The Client represents and warrants, as at the date it accepts this Agreement and again on each occasion that a test, scan, or assessment is initiated under this Agreement, that:

- **(a)** the Client is not incorporated, registered, or established in, and does not have its principal place of business or primary operations in, a Restricted Jurisdiction;
- **(b)** the Tested Entity is not incorporated, registered, or established in, and does not have its principal place of business or primary operations in, a Restricted Jurisdiction; and
- **(c)** the Client is not procuring, and will not use or make available, the Services for or on behalf of any entity that is incorporated, registered, or established in, or that has its principal place of business or primary operations in, a Restricted Jurisdiction.

Continuing obligation. The Client shall notify NIMIS immediately if any warranty in this clause becomes untrue at any time during the term, including as a result of any change in the corporate structure, ownership, place of incorporation, or principal place of business of the Client or any

Tested Entity. NIMIS may suspend or decline to perform any Services where it reasonably believes a warranty in this clause is or may be untrue, without liability to the Client.

Risk allocation. The Client indemnifies NIMIS against all losses, liabilities, fines, penalties, and costs (including reasonable legal costs) arising from or in connection with any breach of this clause. The Client acknowledges that these warranties are a material inducement to NIMIS entering into this Agreement. This indemnity is not subject to the limitation of liability in clause 17.

14. Restrictions on use: no resale, no attacking NIMIS, no unauthorised benchmarking or publication

The Services are licensed to the Client for its **own internal use only**. The Client must **not**, without NIMIS's **prior written approval**:

- resell, rent, lease, sublicense, distribute, or otherwise make the Services available to any third party;
- use the Services to provide testing, managed security, or assessment services to third parties, or on a bureau, white-label, or "as-a-service" basis;
- permit any third party to access or use the Services or the Client's account.

The Client must **not**, whether through the Services or by any other means, **test, scan, probe, penetration-test, attack, disrupt, reverse-engineer, or attempt to discover, exploit, or circumvent any vulnerability in or security control of the NIMIS Services, platform, systems, or infrastructure**, or attempt to gain unauthorised access to them. The right granted under this Agreement is to test the **Client's own verified Targets only** and never NIMIS or its systems. Any such activity is a material breach, is unauthorised access, and may be reported to law-enforcement authorities.

NIMIS operates a separate **Partner Programme** (including co-delivery and white-label arrangements). Any resale, managed-service, or partner use requires a separate written **Partner Agreement** with NIMIS. Any use in breach of this clause is a material breach and unauthorised use of the Services.

Channel obligations. Where NIMIS has approved the Client (a "**Partner**") to resell, sublicense, embed, or otherwise make the Services available to any end customer, the Partner shall:

- **(a)** obtain from each end customer, for NIMIS's benefit, warranties materially equivalent to the Jurisdiction Warranty in clause 13, and pass through and enforce equivalent obligations in its own customer agreements;
- **(b)** not submit, route, initiate, or facilitate any Services where the end customer or the Tested Entity is incorporated, registered, or established in, or has its principal place of business or primary operations in, a Restricted Jurisdiction; and
- **(c)** represent and warrant, on each occasion Services are initiated, that no end customer or Tested Entity for which it procures the Services is connected to a Restricted Jurisdiction as described above, and indemnify NIMIS for any breach of this clause.

Benchmarking, publicity, and publication of results. The Services, their Findings, and their performance are made available for the Client's own internal security and evaluation purposes. The Client must **not**, without NIMIS's **prior written consent**:

- **(i)** conduct, commission, or procure any benchmark, comparative, competitive, or performance assessment of the Services (including of the platform's detection rate, coverage, accuracy, false-positive rate, speed, or results) for the purpose of publication or disclosure to any third party; or
- **(ii)** publish, present, or otherwise disclose to any third party the results of any such assessment, any comparison of the Services or their results against any other product or service, or any performance or benchmark claim about the Services.

This restriction reflects that a Test and its Findings are **point-in-time and scope-dependent** (clause 9) and are readily misrepresented when presented without those limitations, and that the manner in which the Services detect and produce results is **NIMIS's Confidential Information and trade secrets** (clauses 10 and 11). Any benchmark, comparative, or performance result that NIMIS agrees in writing may be published must be generated using a current version of the Services, must be complete, accurate, and not false, misleading, or deceptive, and must fairly present the limitations described in clause 9.

For clarity, this paragraph does **not** limit the Client's right to: (i) use the Findings for its own internal security and compliance purposes under clause 10; (ii) make any disclosure required by law, regulation, a court, or a regulator, or to its professional advisers under a duty of confidence; or (iii) exercise any Non-Excludable Right under clause 19. It also does not prevent a genuine, accurate, and non-misleading account of the Client's own experience of the Services that does not disclose benchmark, comparative, or performance results or NIMIS's Confidential Information.

15. Fees and payment

The Client will pay the Fees for the Services, as presented at the point of purchase and administered through the NIMIS entitlement and billing system. Fees are exclusive of taxes, and the Client is responsible for applicable taxes. Except as required by law, as expressly provided in clause 23(d) (refund on no-fault termination by NIMIS), or as otherwise expressly stated, Fees are **non-refundable**, and unused Tests are not refunded and do not carry over between periods or beyond an access window.

The Services are offered on one-off and subscription plans. Unless the Client's Order Form states otherwise:

- **(a) One-off web-application testing.** A one-off purchase entitles the Client to run a set number of Tests (currently up to **two** complete Tests: an initial test to find vulnerabilities and a second test to confirm the Client's fixes) against the enrolled web application, and remains valid for **90 days from the date of purchase**. Tests not run within that window are forfeited. NIMIS will send a reminder to the account owner in advance of the window closing (currently around **7 days** beforehand) and a further notice when the window ends.
- **(b) Subscriptions.** Subscription plans renew **automatically** each billing period (monthly or annually, according to the plan) on the anniversary of the Client's initial purchase, as administered by the payment provider, and include a set number of Tests per period that do not roll over. Subscriptions continue until cancelled.
- **(c) Cancellation.** The Client may cancel a subscription **at any time**, and is responsible for doing so through the subscription-management facility provided. Cancellation takes effect at the **end of the current billing period**: the subscription does not renew for the next period, access and the Tests included in the current period continue until that period ends, and any separate, unexpired one-off access continues to its own expiry. **Cancellation does not entitle the Client to a refund of Fees paid for the current period or any unused portion of it.** When the Client's last remaining entitlement lapses, clause 15(f) applies (account suspension, then deletion after the grace period).
- **(d) Price.** A subscription renews at the price the Client subscribed to. NIMIS does not apply automatic price increases to an existing subscription; any change to the price of a plan applies only on a new or changed subscription that the Client agrees to.
- **(e) Non-payment.** NIMIS may suspend or withhold the Services for non-payment, in addition to its rights under clause 23.

- **(f) Expiry, retention, and deletion.** When the Client has no remaining entitlement (its one-off window has closed, or its subscription has ended and no other entitlement remains), the account is suspended and, after a limited grace period (currently around **30 days**) during which Findings and reports remain recoverable, the account and its associated data are **permanently and irreversibly deleted**. NIMIS retains billing and tax records, and the record of the Client's acceptance of this Agreement, for as long as required by law.

Tests may be subject to time windows and usage limits associated with the purchased plan.

16. Warranties and disclaimers

Except as expressly stated in this Agreement, and subject to clause 19, the Services and Findings are provided "**as is**" and "**as available**", and NIMIS disclaims all warranties, express, implied, or statutory, including merchantability, fitness for a particular purpose, title, non-infringement, and any warranty that the Services will be uninterrupted, error-free, secure, or will detect all vulnerabilities.

17. Limitation of liability: capped at the cost of the single Test

Subject to clause 19 (Australian Consumer Law):

- **(a) Exclusion of indirect loss.** To the maximum extent permitted by law, neither party is liable for any indirect, incidental, special, consequential, exemplary, or punitive loss, or for loss of profits, revenue, data, goodwill, business, or business interruption, however arising, whether in contract, tort (including negligence), statute, or otherwise, even if advised of the possibility.
- **(b) Liability cap.** To the maximum extent permitted by law, NIMIS's total aggregate liability arising out of or in connection with a Test, a Target, this Agreement, or the Services **will not exceed the Fees paid by the Client for the most recent Test** preceding the event giving rise to the claim. For subscription or multi-Test plans, the Fees attributable to a single Test are taken to be the amount payable for the applicable billing period divided by the number of Tests included in that period.
- **(c) Sole and exclusive remedy.** The remedy in (b) is the Client's **sole and exclusive** remedy against NIMIS, reflects the agreed allocation of risk and the price of the Services, and applies regardless of the number or theory of claims.

- **(d) Savings clause.** If the cap in (b) is held unenforceable or inapplicable for any claim, NIMIS's liability for that claim is limited to the **smallest** amount permitted by the applicable law.
- **(e) Client obligations unaffected.** This clause does not limit the Client's obligations under clause 20 (indemnity) or its liability for breach of clause 5 (authorisation) or clause 14 (restrictions on use).

18. Client status; entire agreement; non-reliance

- **(a) Business acquisition.** The Client represents and warrants that it is entering into this Agreement, and acquiring the Services, **for the purposes of a business, trade, profession, or occupation**, and not as a natural-person consumer for personal, domestic, or household use.
- **(b) Sophisticated party.** The Client represents that it has had the opportunity to obtain independent legal and technical advice, understands the nature and risks of penetration testing, and enters this Agreement on an arm's-length basis.
- **(c) Entire agreement.** This Agreement, together with the applicable Order Form, plan terms, Privacy Policy, and any DPA or Partner Agreement, is the entire agreement between the parties for the Services and supersedes all prior or contemporaneous proposals, representations, and understandings, whether oral or written.
- **(d) Non-reliance.** The Client acknowledges that, in entering this Agreement, it has **not relied** on any representation, warranty, promise, forecast, or statement (including as to security outcomes, coverage, or results) that is not expressly set out in this Agreement. To the maximum extent permitted by law, the Client waives any claim (including in tort or under statute) based on any such representation, **except** for liability arising from fraud or any liability that cannot be excluded by law.

19. Australian Consumer Law

Nothing in this Agreement excludes, restricts, or modifies any consumer guarantee, right, or remedy under the **Competition and Consumer Act 2010 (Cth)** (including the **Australian Consumer Law**) or any other law that cannot lawfully be excluded ("**Non-Excludable Rights**").

The Services are of a kind **ordinarily acquired for business use and not for personal, domestic, or household use**. Accordingly, to the extent permitted by **section 64A of the**

Australian Consumer Law and subject to the Non-Excludable Rights, NIMIS's liability for failure to comply with a guarantee (other than a guarantee under sections 51 to 53 of the Australian Consumer Law) is limited, at NIMIS's option, to:

- resupplying the relevant services, or paying the cost of resupply; and, in the case of goods, replacing or repairing the goods, supplying equivalent goods, or paying the cost of doing so.

To the extent a Non-Excludable Right applies and this clause conflicts with clause 17, this clause prevails only to the minimum extent required by law.

20. Indemnity by the Client

To the maximum extent permitted by law, the Client will indemnify, defend, and hold harmless NIMIS and its officers, employees, contractors, and agents from and against all claims, liabilities, damages, losses, fines, penalties, costs, and expenses (including reasonable legal costs on a full-indemnity basis) arising out of or relating to:

- **(a)** the Client's breach of clause 5 (authorisation and ownership), including any testing of a system the Client did not own or was not authorised to test;
- **(b)** the Client's decision to test a production environment under clause 7;
- **(c)** the Client's breach of clause 13 (Jurisdiction Warranty) or clause 14 (restrictions on use / resale / benchmarking and publication / channel obligations);
- **(d)** the Client's breach of any third-party acceptable-use, hosting, or testing policy;
- **(e)** any claim by a third party (including a data subject, hosting provider, customer, or system owner) arising from a Test the Client authorised or configured;
- **(f)** the credentials the Client provided for testing, or the access those credentials granted; and
- **(g)** the Client's violation of any law or third-party right in connection with the Services.

This indemnity is not subject to the limitation of liability in clause 17.

Conduct of claims. In respect of any claim for which the Client is obliged to indemnify NIMIS under this Agreement (including under clause 13, clause 14, or this clause 20):

- **(i) Notice.** NIMIS will notify the Client in writing of the claim reasonably promptly after becoming aware of it. A failure or delay in giving notice does not relieve the Client of its obligations, except to the extent the Client is materially prejudiced by that failure or delay.

- **(ii) Conduct.** The Client may, by written notice to NIMIS given within **10** business days of NIMIS's notice and conditional on the Client first acknowledging in writing that the claim is subject to its indemnity, assume conduct of the defence and settlement of the claim using legal representatives reasonably acceptable to NIMIS. If the Client does not validly assume conduct, or does not thereafter diligently conduct the defence, NIMIS may defend, settle, or compromise the claim as it sees fit without prejudice to the indemnity, and the Client remains liable for the cost.
- **(iii) NIMIS safeguards.** NIMIS may, at its own cost, participate in the defence with its own legal representatives. NIMIS may instead elect to assume sole conduct of the defence at the Client's expense where the claim: (A) is brought by a regulator or law-enforcement authority, or alleges criminal conduct; (B) involves NIMIS's Confidential Information, trade secrets, or intellectual property; (C) seeks injunctive or other non-monetary relief against NIMIS; or (D) could, in NIMIS's reasonable opinion, materially damage NIMIS's reputation or operations.
- **(iv) Settlement.** The Client must not settle or compromise any claim without NIMIS's prior written consent (not to be unreasonably withheld or delayed) unless the settlement: (A) provides for the unconditional release of NIMIS from all liability; (B) is solely for a monetary payment the Client makes; and (C) imposes no obligation, restriction, or admission of fault or liability on NIMIS.
- **(v) Cooperation.** Each party will give the other reasonable cooperation and information in connection with the defence of the claim; NIMIS's reasonable costs of providing cooperation are covered by the indemnity.

21. Time limit on claims

To the maximum extent permitted by law, any claim or proceeding by the Client arising out of or relating to this Agreement, a Test, or the Services **must be commenced within twelve (12) months** after the date on which the cause of action first accrued. Any claim not commenced within that period is permanently barred. This clause does not apply where the applicable law prohibits such a limitation.

22. Dispute resolution, governing law, and jurisdiction

- **(a) Governing law.** This Agreement is governed by the laws of **the State of Victoria** and the Commonwealth of Australia.

- **(b) Pre-action negotiation.** Before commencing any proceeding (other than for urgent injunctive or interlocutory relief), a party must give written notice of the dispute, and the parties' senior representatives must attempt in good faith to resolve it for at least **30** days.
- **(c) Exclusive jurisdiction.** The parties submit to the **exclusive** jurisdiction of the courts of **Victoria**, and courts competent to hear appeals from them, for any dispute arising out of or relating to this Agreement or the Services. The Client agrees not to commence or maintain any proceeding in any other forum and consents to the stay or dismissal of any proceeding brought contrary to this clause.
- **(d) Waiver of jury trial and class actions.** To the maximum extent permitted by law, each party **waives any right to trial by jury** and **waives any right to commence or participate in any class, collective, consolidated, or representative action** in connection with any dispute arising out of or relating to this Agreement. Disputes must be brought in an individual capacity only.

23. Suspension and termination

- **(a) Termination for cause.** NIMIS may **immediately suspend or terminate** the Services, a Test, or the Client's account if NIMIS reasonably suspects a breach of clause 5 or 14, unauthorised testing, unlawful use, non-payment, or a risk to NIMIS, a third party, or any system.
- **(b) Termination for material breach.** Either party may terminate for the other's material, uncured breach on **30** days' written notice; breaches of clause 5 are not capable of cure.
- **(c) No-fault termination by NIMIS.** NIMIS may also terminate the Services or the Client's account **without cause** (for example, if NIMIS withdraws or discontinues the Services or a plan) on reasonable prior written notice to the account owner.
- **(d) Refund on no-fault termination.** Where NIMIS terminates under clause 23(c), and the termination is **not** attributable to any act, omission, or breach of the Client or to any ground in clause 23(a) or (b), NIMIS will refund to the Client the portion of Fees the Client has paid that is fairly attributable to its **paid, unused, and unexpired** entitlement as at the termination date, calculated on a pro-rata basis using the per-Test amount determined under clause 17(b). **No refund is payable for Tests that have been used, that have expired or been forfeited, or for any entitlement suspended or terminated under clause 23(a) or (b).** This refund is the Client's **sole and exclusive** remedy in respect of a no-fault termination under clause 23(c).
- **(e) Effect of suspension.** Where NIMIS suspends (rather than terminates) the Services or the Client's account under clause 23(a), NIMIS will notify the account owner, and the Client may

seek to resolve the underlying concern. If the suspension is for a ground attributable to the Client (including a breach, unlawful use, non-payment, or unauthorised testing), the Client's access window and entitlement period continue to run during the suspension. If NIMIS determines the suspension was not warranted, NIMIS will restore the Services and extend the affected access window or entitlement period by the duration of the suspension. Suspension does not entitle the Client to any refund except as expressly provided in clause 23(d).

- **(f) Effect of termination.** On termination, the Client's right to use the Services ends. Clauses that by their nature survive (including 5, 7–14, 15 (accrued Fees and clause 15(f) retention and deletion), 16–22, and 24) survive termination.

24. General

- **Order of precedence.** In case of conflict: (1) a signed Master Services Agreement or Order Form; (2) this Agreement; (3) the general Terms of Service.
- **Variation.** NIMIS may update this Agreement; material changes take effect on posting a new version with a revised date, and continued use constitutes acceptance. **The version accepted at the time of a Test governs that Test**, and NIMIS records the accepted version, timestamp, and account identifier.
- **No modification except in writing.** No variation by the Client is effective unless agreed by NIMIS in writing.
- **Assignment.** The Client may not assign or novate this Agreement without NIMIS's prior written consent. NIMIS may assign it in connection with a corporate transaction.
- **Force majeure.** Neither party is liable for delay or failure to perform (other than an obligation to pay money) caused by events beyond its reasonable control. The affected party will notify the other as soon as reasonably practicable, use reasonable efforts to mitigate the effect of the event, and resume performance promptly once able. If a force majeure event materially prevents performance for a continuous period of more than **60** days, either party may terminate this Agreement on written notice, in which case clause 23(d) applies to any prepaid, unused, and unexpired entitlement as if NIMIS had terminated without cause.
- **Severability / waiver.** If any provision is unenforceable, it is read down or severed to the minimum extent necessary and the remainder stands; no failure or delay in enforcing a provision is a waiver of it.
- **Relationship.** The parties are independent contractors; nothing creates a partnership, agency, employment, or joint venture.

- **Notices.** Legal notices to NIMIS may be sent to **legal@nimisintelligence.com**; operational queries, including requests relating to a Test in progress, may be sent to **ops@nimisintelligence.com**. Notices to the Client may be sent to the account or billing contact on file. A notice sent by email is deemed received on the day it is sent if that day is a business day and it is sent before **5:00pm** in the recipient's local time, and otherwise on the next business day, provided the sender does not receive an automated delivery-failure notification.
-

By accepting this Agreement, enrolling an application, or running a Test, the Client acknowledges that it has read, understood, and agrees to be bound by this Agreement, including the authorisation warranties (clause 5), the production-testing risk allocation (clause 7), the acknowledgment and assumption of risk (clause 8), the point-in-time limits of testing (clause 9), the Jurisdiction Warranty (clause 13), the restrictions on use, benchmarking, and publication (clause 14), the limitation of liability (clause 17), and the dispute-resolution and waiver provisions (clause 22).

Accepted version, timestamp, and account identifier are recorded by NIMIS at the time of acceptance.